JUSTITSMINISTERIET

Folketinget
Retsudvalget
Christiansborg
1240 København K

Dato: 27. juni 2013
Kontor: Sikkerheds- og Forebyggelseskontoret
Sagsbeh: Linda Björk Nielsen
Sagsnr.: 2013-0030-1509
Dok.: 801562

Hermed sendes besvarelse af spørgsmål nr. 904 (Alm. del), som Folketingets Retsudvalg har stillet til justitsministeren den 7. juni 2013. Spørgsmålet er stillet efter ønske fra Peter Skaarup (DF).

Morten Bødskov

/

Anette Arnsted

Slotsholmsgade 10
1216 København K.

Telefon 7226 8400
Telefax 3393 3510

www.justitsministeriet.dk
jm@jm.dk

Spørgsmål nr. 904 (Alm. del) fra Folketingets Retsudvalg:

> ”Vil ministeren i forlængelse af REU alm. del spørgsmål 896 oplyse, hvornår hhv. Rigspolitichefen, Justitsministeriet og Økonomi- og indenrigsministeren første gang blev orienteret om hackerangrebene på de centrale computere hos CSC, og hvilke initiativer tog hhv. Rigspolitiet og Justitsministeriet i forlængelse af orienteringerne?”

Svar:

Justitsministeriet har til brug for besvarelsen indhentet udtalelser fra Rigspolitiet og Politiets Efterretningstjeneste.

Rigspolitiet har oplyst følgende:

> ”Det bemærkes indledningsvis, at Rigspolitiets bidrag til brug for Justitsministeriets besvarelse tager udgangspunkt i Rigspolitiets viden på nuværende tidspunkt. Det understreges i den forbindelse, at der er tale om en igangværende efterforskning. Der er tale om enorme datamængder, som dansk politi løbende modtager fra svensk politi og herefter analyserer. Disse undersøgelser pågår fortsat, hvorfor det ikke kan udelukkes, at billedet senere ændrer sig.
>
> Rigspolitiet kan oplyse, at en svensk statsborger ultimo august 2012 blev anholdt i Cambodja, hvorefter pågældende blev udleveret til Sverige og fængslet primo september 2012 i forbindelse med efterforskningen af en sag om hacking samt til afsoning af en svensk dom på 1 års fængsel for krænkelse af ophavsretsloven.
>
> Rigspolitiet var herefter i dialog med svensk politi om en del af den svenske efterforskning, der blandt andet omhandlede hacking af et pengeinstituts it-systemer. Oplysninger pegede på, at også danske konti i pengeinstituttet havde været anvendt til kriminalitet i den sammenhæng. Endvidere orienterede svensk politi om, at den foreløbige datagennemgang viste, at også danske internethjemmesider mv. kunne være forsøgt hacket.
>
> Medio januar 2013 sendte svensk politi uddrag af en række logfiler, som svensk politi var kommet i besiddelse af i forbindelse med deres efterforskning. Herved modtog dansk politi for første gang data, der viste, at CSC, herunder politiets data, kunne være kompromitteret af den svenske statsborger. Dette blev dog ikke umiddelbart konstateret i forbindelse med modtagelsen, idet Rigspolitiets Nationale IT-efterforskningssektion (NITES) i denne periode efterforskede flere meget store sager, hvorfor det ikke på dette tidspunkt var muligt at allokere res-

sourcer til en gennemgang af materialet, og der blev på den baggrund ikke på dette tidspunkt foretaget en nærmere undersøgelse af materialet. En gennemgang af materialet modtaget fra svensk politi blev således først foretaget ultimo februar 2013. Det kunne på baggrund af denne gennemgang konstateres, at der havde fundet uautoriseret adgang sted til politiets data fra et mainframesystem hos CSC Danmark A/S (CSC), som har kontrakt med en lang række offentlige myndigheder samt nordiske private virksomheder om at varetage behandlingen af centrale it-systemer, herunder en del af dansk politis registre mv.

Der blev straks herefter afholdt et møde mellem Rigspolitiet og CSC, hvor det blev aftalt, at der med det samme skulle iværksættes en nærmere undersøgelse hos CSC med deltagelse af Rigspolitiets Koncern-IT og NITES for hurtigst muligt at identificere den nærmere karakter af sårbarheden i systemet med henblik på at sikre, at denne blev lukket.

I perioden herefter har der været løbende dialog mellem Rigspolitiet og CSC. Rigspolitiet anmodede primo marts 2013 skriftligt CSC om en redegørelse samt sikring af data med henblik på efterforskning. CSC afleverede flere rapporter til Rigspolitiet om hændelsen. I den forbindelse oplyste CSC Rigspolitiet om, at den sårbarhed i systemet, som havde været benyttet til at opnå uautoriseret adgang, var identificeret og lukket, samt at der var identificeret og fjernet såkaldte ”bagdøre” til systemet. CSC oplyste endvidere, at der ikke var fundet tegn på, at der havde været direkte adgang til Kriminalregisteret eller andre registre på systemet. Det var endvidere CSC’s vurdering, at det med stor sandsynlighed kunne udelukkes, at der var ændret, tilføjet eller slettet oplysninger i registrene.

Rigspolitiet iværksatte i samarbejde med uvildige eksterne iteksperter en supplerende selvstændig undersøgelse med henblik på bl.a. at verificere CSC’s oplysninger. Sideløbende hermed fortsatte Rigspolitiet undersøgelserne af det særdeles omfattende tilvejebragte materiale.

Herudover indledte Københavns Politi bistået af efterforskere fra NITES primo marts 2013 en strafferetlig efterforskning.

Som led i undersøgelserne samarbejdede Rigspolitiet løbende med svensk politi om at få udleveret relevant materiale fra den svenske efterforskning. Primo april 2013 modtog Rigspolitiet en CD-rom med en pakket fil sikret fra den svenske statsborgers computer i forbindelse med anholdelsen. Rigspolitiet iværksatte straks efter modtagelse en undersøgelse af materialet og sammenholdt det med oplysninger fra CSC. Det konstateredes, at filen bl.a. indeholdt en række talkoder og navne på fortrinsvis udenlandske statsborgere. En nærmere analyse i de

efterfølgende uger af oplysningerne viste, at der var tale om ca. 1,2 millioner såkaldte "records" vedrørende efterlysninger i Schengen-informationssystemet (SIS).

Rigspolitiet får løbende i forbindelse med undersøgelserne, der stadig pågår, gradvis øget indsigt i omfanget og karakteren af den svenske statsborgers aktiviteter på mainframen hos CSC, og Rigspolitiet vurderede medio maj at have den fornødne klarhed over det passerede.

På den baggrund orienterede Rigspolitiet den 17. maj 2013 telefonisk Datatilsynet om sikkerhedsbristen. Den 21. maj 2013 orienterede Rigspolitiet endvidere Justitsministeriet telefonisk om sagen og sendte den 24. maj 2013 en notits til Justitsministeriet herom.

Den 29. maj 2013 orienterede Rigspolitiet Justitsministeriet om, at undersøgelserne havde vist, at der havde været aktivitet mod CPR-registerets miljø på mainframen fra politiets miljø på mainframen den 8. april 2012. Herefter underrettede Rigspolitiet den 30. maj 2013 efter aftale med Justitsministeriet telefonisk Økonomi- og Indenrigsministeriet herom, ligesom Datatilsynet på ny blev telefonisk orienteret om sagen den 31. maj 2013.

Den 31. maj 2013 afsagde Københavns Byret fængslingskendelse med henblik på udlevering af den svenske statsborger til Danmark.

Rigspolitiet orienterede den 3. juni 2013 Kommissionen om sagen i relation til oplysningerne i SIS.

Den 5. juni 2013 foretog Københavns Politi anholdelse af en formodet dansk medgerningsmand. Endvidere blev der foretaget ransagning på flere adresser.

Dagen efter, den 6. juni 2013, blev den formodede danske medgerningsmand fremstillet i grundlovsforhør for lukkede døre og varetægtsfængslet i foreløbig 4 uger.

Rigspolitiet, Politiets Efterretningstjeneste og Københavns Politi orienterede ved et fælles pressemøde samme dag offentligheden om sagen.

Rigspolitiet udsendte endvidere samme dag en note vedrørende sikkerhedsbristen til Schengen-landene, Rådssekretariatet og Kommissionen, ligesom Den Europæiske Tilsynsførende for Databeskyttelse blev orienteret om sagen. Det kan i forlængelse heraf oplyses, at Rigspolitiet den 26. juni 2013 deltager i et møde med Schengen-landene, sikkerhedseksperter for EU-agenturer og Europol samt Den Europæiske Tilsynsførende for

Databeskyttelse, hvor Rigspolitiet på ny vil orientere om sagens forløb og udvikling samt indgå i drøftelser i forhold til fremadrettede sikkerhedstiltag.

På baggrund af sagen overvejer Rigspolitiet nøje, hvilke initiativer der måtte være behov for at iværksætte i forhold til it-sikkerheden omkring politiets registre. Dette sker i tæt samarbejde mellem Rigspolitiet, PET og andre aktører."

Politiets Efterretningstjeneste har til brug for Justitsministeriets besvarelse udtalt følgende:

"Politiets Efterretningstjenestes (PET) opgave er at forebygge, efterforske og modvirke foretagender og handlinger, der udgør eller vil kunne udgøre en fare for Danmark som et selvstændigt, demokratisk og sikkert samfund. PET skal gennem sin virksomhed skabe grundlag for, at trusler af den nævnte karakter kan identificeres og håndteres så tidligt og effektivt som muligt. I den forbindelse har PET blandt andet fokus på, om der er grupper eller personer, som benytter strafbare metoder - f.eks. ved at skaffe sig adgang til oplysninger i offentlige registre, herunder politiets registre - for at nå politiske eller ideologiske mål.

PET er tillige national IT-sikkerhedsmyndighed for Justitsministeriets område, herunder politi og anklagemyndighed. I den egenskab udøver PET kontrol med, at reglerne i Statsministeriets cirkulære nr. 204 af 7. december 2001 vedrørende sikkerhedsbeskyttelse af informationer af fælles interesse for landene i NATO, EU eller WEU, andre klassificerede informationer samt informationer af sikkerhedsmæssig beskyttelsesinteresse i øvrigt (sikkerhedscirkulæret) overholdes.

PET udøver sin funktion som IT-sikkerhedsmyndighed gennem løbende rådgivning af politi og anklagemyndighed. PET godkender endvidere IT-systemer, hvorpå klassificerede oplysninger opbevares og behandles.

Det mainframe-anlæg hos CSC, som har været udsat for hackerangreb, behandler ikke klassificerede oplysninger og er dermed ikke omfattet af reglerne i sikkerhedscirkulæret og følgelig heller ikke omfattet af PET's godkendelses- og kontrolvirksomhed.

PET blev den 5. juni 2013 af Rigspolitiet bedt om at forestå en undersøgelse af sagen om hackerangrebet mod CSC. Undersøgelsen har til formål dels at afdække omfanget af og årsagerne til sikkerhedsbruddet, dels at fremkomme med fremadrettede sikkerhedsanbefalinger.

> PET er i løbende dialog med politi og anklagemyndighed om håndtering af følsomme oplysninger, og PET tog i 2011 initiativ til et projekt, der har til formål at sikre et passende og ensartet beskyttelsesniveau for følsomme oplysninger, der behandles og opbevares i regi af politi og anklagemyndighed. Projektet er forankret i Rigspolitiet. PET har løbende bidraget med ekspertviden og rådgivning til projektet, og de indledende anbefalinger er forelagt Rigspolitiets direktion i foråret 2013.
>
> PET har endvidere iværksat en kortlægning af, hvorledes trafikmonitering og logning på politiets og anklagemyndighedens IT-systemer kan styrkes.
>
> PET har et tæt samarbejde med Københavns Politi om efterforskningen af hackerangrebet mod CSC og sikrer blandt andet i den forbindelse, at der så vidt muligt tilgår efterforskningen de fornødne kapaciteter og kompetencer. PET yder ligeledes bistand med henblik på at afdække aspekter i sager, der kan have betydning for den nationale sikkerhed, ligesom PET løbende sikrer, at efterretningstjenestens oplysninger, som kan have betydning for sagen, inddrages i efterforskningen. PET kan ikke inden for rammerne af en folketingsbesvarelse redegøre nærmere for denne bistand."

Justitsministeriet kan i øvrigt oplyse, at der i politiet og anklagemyndigheden er iværksat et projektarbejde om indsatsen på cyberområdet. Rigspolitiet, PET og Rigsadvokaten arbejder således i fællesskab på et projekt om, hvordan politiet og anklagemyndigheden håndterer de udfordringer, som udviklingen på IT-området skaber i forhold til bl.a efterforskning og retsforfølgning af cyberkriminalitet. Projektet skal også danne grundlag for en ordning, som sikrer, at relevante oplysninger modtages fra og afgives til Forsvarets Efterretningstjeneste, Center for Cybersikkerhed, der uden for Justitsministeriets område er Danmarks nationale it-sikkerhedsmyndighed.